Disability services. Putting you first.

Privacy Policy and Practice Manual

Table of Contents

Privacy Policy **3**

Practice Information **4**

1 Responsibilities 4

2 Definitions 4

3 Privacy Statement 5

4 Privacy Guidelines and Practices 7

5 Aruma's response to APP's: 7

APP 1: Openness and Transparency **7**

APP 2: Anonymity and pseudonymity **8**

APP 3: Collection of information (solicited) **8**

APP 4: Collection of information (unsolicited) **10**

APP 5: Notifications **10**

APP 6: Use and Disclosure **11**

APP 7: Direct Marketing **13**

APP 8: Cross border disclosures **14**

APP 9: Government identifiers **15**

APP 10: Data quality (Quality of Personal Information) **15**

APP 11: Data security (Security of Personal Information) **16**

APP 12: Access **17**

APP 13: Correction of Personal Information 18

6 APP Exemptions 19

7 Other Privacy Practice Guidelines 20

Resources Relevant to this Policy and Practice Manual **23**

8 QMS policies, procedures and/or forms 23

9 Legislation, external requirements and oversight bodies 23

10 External resources 23

Privacy Policy

1. Aruma oversees and manages the privacy of personal information and adopts a 'good privacy practice' approach to information collection, use and disclosure, security of personal information, and upholding individuals' right to access and correct their information.

2. Aruma will comply with, and exceed, its obligations under the Privacy Act 1988 (Cth) (the Privacy Act), the associated 13 Australian Privacy Principles (APPs), and various Commonwealth and State legislations.

3. This policy sets out how Aruma fulfils its obligations in relation to the privacy of personal information.

4. We will:

   - Use all reasonable endeavours to ensure that personal information is only collected and used for the intent of collection, stored and managed in a secure way, and disclosed under the guidelines of the APPs.

     This includes, but is not restricted to, personal information on customers, employees, carers, contractors, volunteers, donors and other stakeholders, which is collected through various stages of engagement.

     This information can be from a one-off dealing or cover an extensive period of time and cross over all aspects on the individual's life including, but not limited to, financial, health and wellbeing, behaviour management, self-care, personal history, relationships, goals and aspirations and educational and training.

   - Ensure people understand their rights under the Privacy Act. This includes:

     - knowing what information Aruma holds about them;
     - being provided with information regarding the collection, use, disclosure and storage of the information; and
     - correcting that information if it is out of date or inaccurate.

   - Have in place clear, up to date and easy to access policies and procedures to make sure that the APPs are complied with, and that questions and complaints about the APPs are dealt with.

5. This policy and the associated APPs apply to all levels of employees across all levels of our group. All employees, carers, contractors and volunteers within Aruma have a responsibility to make sure personal information is handled in a way that complies with this policy.

6.

Practice Information

1 Responsibilities

1.1 The application of the Privacy Policy and Practice Manual and associated Privacy Principles rests with all level of employees across all levels of our group.

1.2 All employees, carers, contractors and volunteers within Aruma have a responsibility to make sure personal information is handled in a way that complies with this policy.

1.3 All employees are required to sign a 'Code of Conduct', which includes a commitment to upholding privacy and confidentiality, on commencement of employment and re-commit to the code each year during annual performance reviews.

2 Definitions

Chief Privacy Officer: Aruma has a Chief Privacy Officer. The role of the Chief Privacy Officer is to:

- receive and answer any requests for access to, or correction of, personal information;
- accept and answer any concerns, complaints or alleged breaches about privacy issues; and
- be the contact for the Australian Information Commissioner in relation to any privacy issues.

Personal Information: (as defined in the Privacy Act) means information or an opinion about an identified or reasonably identifiable individual, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not. Personal Information can include photos and images, video or other recordings, electronic information, paper based, written communication including letters and emails and is generally referred to under two categories:

- **Sensitive information**: means personal information about a person's:
  - racial or ethnic origin;
  - political opinion or membership of a political association;
  - trade union or professional association membership;
  - religious beliefs or affiliations or philosophical beliefs;
  - sexual orientation or practices;
  - criminal record;

- genetic information; or
- biometric information or templates.

- **Health information**: can be actual or opinion about the health (including an illness), disability or injury of an individual, about an individual's expressed wishes about the future provision of health services to them or about a health service provider or to be provided.

Aruma holds various types of personal information on customers, employees, carers, contractors, volunteers, donors and other stakeholders, collected through various stages of engagement. This information can be from a one-off dealing or cover an extensive period of time and cross over all aspects of the individual's life, including but not limited to financial, health and wellbeing, behaviour management, self-care, personal history, relationships, goals and aspirations and education and training.

Permitted General Situation: is a circumstance in which a collection, use or disclosure of personal information is permitted and generally covers threat to life, health or safety; unlawful activity or serious misconduct; missing persons; legal or equitable claims; and alternative dispute resolution.

Reasonable Steps: are steps that are reasonable in the circumstances and taken in view of relevant considerations, such as the sensitivity of the information and what a reasonable individual would expect. This assessment should be made on a case-by-case basis.

Records and Forms: The Privacy Principles apply to all information that is held as a record, including a document, database (including CRM systems), photograph or other pictorial representation of a person. Information should only be retained and stored (forming a record) that is necessary for the provision of service or ongoing business dealings.

Consent (APP Key Concept): The main issue of consent rises for purposes of disclosure. The APPs permit various collections, uses and disclosures where they are **with consent**. Consent can be either express (by way of signed form) or implied (verbal).

Breach or Possible Breach (VIC): an action or omission that results in loss, theft, misuse or unauthorised disclosure of personal information or has the potential to do so.

Near Miss (VIC): situations where a breach would have occurred without intervention. This includes situations where a privacy incident has occurred without any actual disclosure of personal information.

3 Privacy Statement

3.1 Throughout all of Aruma's group of entities, we respect your privacy. We have developed our Privacy Policy in line with the Australian Privacy Principles and other relevant state legislations.

3.2 Our Privacy Policy is available on Aruma's website www.hwns.com.au or you can request a

copy from us.

3.3 Arumas' Privacy Policy tells you about:

- the kinds of personal information that we may collect and hold;
- how we collect and hold personal information;
- the reasons why we collect, hold, use and disclose personal information;
- how you may access the personal information that we hold about you;
- how you can ask for your personal information to be changed if it is incorrect; and
- how you can ask questions or make a complaint about how Aruma has handled your personal information.

3.4 Here is a summary of some important aspects of our Privacy Policy.

3.5 In order to provide services and supports and to conduct our business activities, Aruma may need to collect personal information about you. This may include your name, home and email addresses, date of birth or other defining factors and your telephone numbers. We may also collect some sensitive information such as information about your health or finances.

3.6 If the information we request is not provided, we may not be able to supply you with the services you request.

3.7 We take all reasonable steps to ensure the personal information we collect about you is accurate, relevant, up-to-date, secure and that it is not accessed or disclosed to anyone without authority. We will only disclose your information to people within our organisation who may need to know that information to provide you with the best services. We only do this in ways that comply with the Australian Privacy Principles.

Complaints about Privacy

3.8 Please contact our Chief Privacy Officer if you:

- have any enquiries regarding our Privacy Policy;
- wish to access or correct your personal information;
- require more details about how we handle your personal information; or
- wish to make a complaint about how we have handled your personal information.

Chief Privacy Officer

Aruma

49 Blackbutts Road Belrose NSW 2085

PO Box 93, Frenchs Forest NSW 1640

P: 02 9451 1511 F: 02 9452 5932

privacy@aruma.com.au

4 Privacy Guidelines and Practices

Overview

4.1 The *Privacy Act 1988* (Privacy Act) regulates how personal information is handled by the not-for-profit sector, and various other agencies.

4.2 The Office of Australian Information Commissioner (OAIC) deals with issues covered by the Privacy Act (Cth) 1988.

4.3 The following guidelines and practices set out how Aruma of entities, including Aruma (Aruma) uses, discloses and secures personal information and how we provide individuals with a right to access and correct their information in line with the Australian Privacy Principles (APP).

5 Aruma's response to APP's:

5.1 APP 1: Openness and Transparency

5.1.1 The objective of APP 1 is to ensure that APP entities manage personal information in an open and transparent way. An APP entity must:

- take steps *to implement practices, procedures and systems to:*
    - *ensure that it complies with the APPs; and*
    - *enable it to deal with inquiries or complaints regarding its compliance with the APPs; and*
- *have a clearly expressed and up to date policy about the management of personal information and must make the policy available.*

Aruma's Practice Guidelines:

Aruma have implemented policies, practices and procedures to ensure both compliance with the APPs, and to deal with inquiries and complaints with regards to the APPs.

Aruma have a clear, up to date and readily available policy statement about its management

of personal information.

Our Privacy Statement is available on Aruma's website www.aruma.com.au.

5.2 APP 2: Anonymity and pseudonymity

5.2.1 The objective of APP 2 is that Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity. This applies unless it is not practical for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

5.2.2 Generally, where an entity has no need to contact the individual in the future, anonymity would likely be appropriate. Where an entity will need to contact the individual again and some form of identifier, but no personal information, is required, pseudonymity would likely be appropriate.

Aruma's Practice Guidelines:

Aruma provides anyone it deals with, the opportunity to keep their name secret (remain anonymous) or to use a false name (pseudonym), except where it is not practical to do so.

5.3 APP 3: Collection of information (solicited)

5.3.1 APP 3 applies to the collection of personal information that is solicited by an APP entity.

5.3.2 Information collected about any individual during any course of dealings should be reasonably necessary for the function or activity of the purpose collected. Information is not necessary merely because it might be useful in the future and as such collection should only be made of information required to deliver a service or activity.

5.3.3 An organisation must not collect:

- *personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities;*
- *sensitive information unless:*
  - *the individual consents to the collection of the information; and*
  - *the information is reasonably necessary for one or more of the entity's functions or activities; or*
  - *the collection of the information is required or authorised by law; or*
- *a permitted general situation exists in relation to the collection of the information; or*
- *a permitted health situation exists in relation to the collection of the information; or*
- *the APP entity is a non-profit organisation and the information relates to the activities of the organisation and the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.*

5.3.4 Personal information must be collected directly from the individual concerned (as opposed to a third party), unless it is unreasonable or impracticable to do so.

5.3.5 Collection of information must be by lawful and fair means (that is without intimidation or deception) and by means that are not unreasonably intrusive.

Aruma's Practice Guidelines:

The personal information that Aruma may request from a person will depend on the type of relationship the person has with any entity within Aruma, for example, whether the person is supported by any entity of Aruma or is an employee, carer, volunteer or donor.

It is Aruma's usual practice to collect personal information directly from the person.

Where a person is not able to provide the information, Aruma may collect the information from another person who has legal responsibility or advocates for the person.

Sometimes Aruma collects personal information from a third party or a publicly available source. This only takes place if the person has agreed to it being collected (consented); would expect us to collect their personal information in this way; or if it is a necessary collection to enable Aruma to provide a service to that person.

Aruma only collects personal information for purposes directly related to our activities, such as:

- providing services and support;
- working with government and other non-government agencies;
- operating our businesses;
- fundraising;
- responding to enquiries about our programs and services; and
- administrative activities.

Aruma may also collect personal information in its normal communications, including when a person:

- emails;
- phones; or
- provides us with their business card.

These records may be stored in our history logs.

Collected information may include name, address, emergency contact details, cultural background, medical and disability information, behaviour management strategies, personal care information and other necessary information to ensure the health, safety and wellbeing

of our employees and customers.

Aruma only collects sensitive information with the consent of the individual:

- when the information directly relates to the activities of the organisation; and
- the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Aruma does not sell, loan or give away any information we collect.

5.4 APP 4: Collection of information (unsolicited)

5.4.1 AAP 4 establishes that if an AAP entity receives unsolicited personal information, it must, within a reasonable period, determine whether or not it could have collected the information if it were so solicited and if so may continue to hold the information and treat in the same manner as collected information under APP 3. If not, the entity must destroy or de-identify it unless it is not lawful to do so.

Aruma's Practice Guidelines:

There are some circumstances where Aruma may receive personal information that it has not asked for (unsolicited information). When this happens, Aruma will decide whether or not we could have collected the information from that person if we had asked.

Where unsolicited personal information is received, Aruma will determine, within a reasonable period of time, if such information is necessary to the continuation of dealings, and where not necessary must destroy or de-identify the information.

5.5 APP 5: Notifications

5.5.1 APP 5 requires entities to provide a privacy collection notice (or privacy statement) when collecting personal information addressing matters such as how and why the information is being collected.

Aruma's Practice Guidelines:

Before, at the time of, or as soon as possible after Aruma collects personal information, it takes steps to tell or make sure that the person whom it is about, is aware why the information is required, what it will be used for, and of how they can access Aruma Privacy Statement or full policy document.

Access to Aruma's privacy statement is provided on our main group website at www.aruma.com.au.

Forms collecting personal information shall have a footnote noting Aruma's compliance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs). Following is an example of a suitable footnote:

"Aruma adheres to the Australian Privacy Principles (2012) and has a Privacy Policy in place to keep your information safe. Personal information collected or received will be used, stored and disposed of as provided for in the Privacy Act 1988 (Cth) and associated Australian Privacy Principles. Read the full Privacy Policy online at hwns.com.au/privacy."

5.6 APP 6: Use and Disclosure

5.6.1 APP 6 sets out the purposes for which personal information may be used and disclosed. Entities are only authorised to use or disclose personal information for the primary purpose for which it was collected.

*5.6.2 The **use** of personal information occurs where the information is handled **internally** within an entity.*

*5.6.3 **Disclosure** occurs where information is sent to a third party **outside** the entity. Disclosure does not include providing information to the individual to whom it relates as this is providing "Access" (APP 12).*

Aruma's Practice Guidelines:

Use of personal information

Aruma only holds personal information for the primary purpose it was given to us.

Use of collected personal information will only occur within Aruma of operations, and will not be used or disclosed to anyone else for a secondary purpose unless one of the following applies:

- The person has agreed (given consent – see below);
- The person would expect Aruma to use or disclose the personal information for the secondary purpose, as it relates to the primary purpose (such as disclosure to NDIA for plan reviews);
- It is required or authorised by law;
- A permitted general situation exists (see s.16A of the Privacy Act);
- A permitted health situation exists (see s.16B of the Privacy Act), in which case steps must be taken to de-identify the information before it is disclosed; or
- Aruma believe that the use or disclosure of the information is necessary for an enforcement related activity (e.g.: Federal Police, Immigration, ATO).

In using personal information during the course of operations, only information sufficient to meet the purpose of the outcome to be achieved will be shared, and only with those involved in achieving the outcome, that is, information will only be shared on a needs-to-know basis.

Disclosure of personal information to a third party

Requests for release or disclosure of personal information to a party other than the individual, should be made to privacy@aruma.com.au

Aruma may only disclose personal information for a particular purpose provided **consent** is first obtained or the individual would reasonably expect disclosure for that purpose and the purpose is related to the reason of collection.

Aruma follows good privacy practices and seeks express consent wherever possible (that is: written or completion of a Consent Form) prior to the disclosure of any personal information.

Collection of data at the time of new engagement with Aruma would be implied, for the purpose of collection.

On receipt of request for release of personal information Aruma will provide acknowledgement of the request and where possible provide a timeframe for providing such information, or reason why disclosure will not be granted.

Aruma may impose a fee to cover costs of photocopying or file extraction dependent on the volume required and ease of access to the data. Such fees, where imposed, will be on a cost basis.

Consent for third party access to information in SIL-Support Services

Customers will be notified at time of engagement with Aruma what information may be shared and with who, and may be asked to consent to regular sharing of certain information – this is called 'blanket consent'. Blanket consent must only be obtained where the disclosure of information can be explicitly defined and must be made clear to the individual what their consent covers.

'Blanket consent' should be updated annually, and would cover regular dealings where personal information is required to be shared, in cases such as:

- sharing of personal information with a doctor or medical practitioner whilst being supported to attend scheduled visits – but not specific medical issues;
- sharing personal information that has been collected over time when engaging at a future time with NDIS during plan reviews, regarding types of support being provided;
- access to personal information held in customer support files by a Community Visitor; and
- where it is not appropriate to obtain blanket consent, and in each case of separate information disclosures, specific consent will be obtained for each instance of information disclosures. Examples of specific consent would be:
    - request for access to incident reports;
    - talking to a specialist on your behalf about a new medical problem; and

- collecting information of photographs of you to use as a good-news story in Aruma marketing.

In assisting a Customer of any of Arumas' entities understand the need for consent, referral should be made to Sharing Information Toolkit and associated documents.

Consent in either form (express or implied) may be revoked at any time.

Release of information without consent to a party external to Aruma (i.e. disclosure) is permitted in circumstances where Aruma reasonably believe it is necessary to lessen or prevent a serious threat to the life, health or safety of an individual. For example, it would be reasonable to release certain information without consent in event of a customer or employee requiring urgent transportation to hospital or in event of a missing person.

De-identification prior to release

De-identified information can still be personal information. An individual's identity can often still be reasonably ascertained from information that does not state their name, for example:

- by matching it with other information that identifies them (e.g. matching an account ID with the account holder's name); or
- where the person's identity is evident from the context in which information is given.

Where a request is received for release of personal information, all 'other' names or identifying details other than that of the person who consented to the release, should be redacted from the data prior to release, unless explicit consent is obtained from each of the other individuals able to be identified.

Approval for release of information

Prior to release of any personal information to a third party, Aruma's Chief Privacy Officer will review data to be released and provide approval once satisfied appropriate redaction has occurred.

5.7 APP 7: Direct Marketing

5.7.1 APP 7 regulates when personal information can be used and disclosed for direct marketing. The requirements can be onerous and relatively restrictive. APP 7 has a major impact on organisations' marketing activities. It regulates matters such as:

- *what information can be used for direct marketing;*
- *notices that must be provided;*
- *consents that must be obtained; and*
- *the provision of unsubscribe facilities.*

5.7.2 Direct Marketing generally includes that directed at specific individuals, for example via: mail, email, facsimile or phone, or door-to-door selling.

Aruma's Practice Guidelines:

Aruma will not use or disclose personal information for use in direct marketing, except where a person has agreed to the use.

Requests for an individual to not receive direct marketing from Aruma can be made via privacy@hwns.com.au

Although there is a journalism exemption in place (See section below on 'Exemption – Newsletters') Aruma will seek express consent from each person about whom 'publicity or good-news stories' are about at the time of collection (including photographic images). Aruma will take all endeavours to ensure the individual is made aware of all possible uses of the information and/or image collected.

Consent for use of personal information or images in Aruma's marketing may be revoked at any time by the individual by writing to Aruma's Privacy Officer.

5.8 APP 8: Cross border disclosures

5.8.1 AAP 8 only applies to disclosure of information to an overseas third party. Before an APP entity discloses personal information about an individual to a person who is not in Australia, it must take steps to ensure that the overseas recipient does not breach the APPs in relation to the information.

Aruma's Practice Guidelines:

If Aruma is to disclose personal information to any overseas recipient, the overseas recipient must consider and comply with, the terms of this APP.

Aruma may only disclose personal information to an overseas recipient in the following circumstances:

- The overseas entity/person can demonstrate they respond to a law that can protect the information in a way that is similar to the APP's;
- The individual agrees to the disclosure (gives consent) after being informed of the principles of AAP 8 – Cross border disclosures;
- The disclosure of the information is required by law or under an inter-Australian agreement;
- A permitted general situation exists (see s.16A of the Privacy Act); or
- Aruma believes that the disclosure of the information is necessary for enforcement related activities.

5.9 APP 9: Government identifiers

5.9.1 The principle of AAP 9 is that an organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless the adoption of the government related identifier is required or authorised by, or under, an Australian law or a court/tribunal order.

5.9.2 *An organisation must not use or disclose a government related identifier of an individual unless:*

a. it is necessary for the organisation to verify the identity of the individual;

b. it is necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority;

c. it is required or authorised by or under an Australian law or a court/tribunal order;

d. a permitted general situation exists;

e. the organisation believes it is necessary for an enforcement related activity conducted by, or on behalf of, an enforcement body; or

f. unless prescribed by the regulations.

Aruma's Practice Guidelines:

Aruma will NOT adopt a government related identifier of a person (e.g. Medicare, driver's licence, NDIS number) as its own identifier, nor will it disclose a government related identifier of the person unless:

- it is necessary for Aruma to verify the identity of the person;
- it is necessary for Aruma to fulfil its obligations to an agency or State or Territory authority;
- it is required by law or court/tribunal order;
- a permitted general situation exists (see s.16A of the Privacy Act); or
- Aruma believes it is necessary for an enforcement related activity.

5.10 APP 10: Data quality (Quality of Personal Information)

5.10.1 APP 10 aims to ensure personal information that an entity holds about an individual is accurate to ensure he or she does not suffer any unfair consequences of action taken, based on inaccurate information.

5.10.2 An entity must take reasonable steps to ensure that the personal information it:

- ***collects** is accurate, up to date and complete; and*

- ***uses or disclosures*** *is accurate, up to date, complete and relevant.*

Aruma's Practice Guidelines:

Aruma takes reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, up to date and complete.

These steps include maintaining and updating personal information when we are advised by a person that their personal information has changed.

5.11 APP 11: Data security (Security of Personal Information)

5.11.1 APP 11 requires an entity that holds personal information to ensure that it is stored and handled ***securely****.*

5.11.2 An entity must take reasonable steps to protect personal information against:

- *misuses,*
- *interference,*
- *loss, and*
- *unauthorised access, modification and disclosure.*

Arumas' Practice Guidelines:

Aruma takes steps to ensure the personal information it holds is stored in a manner so that it cannot be misused, interfered with, lost, accessed by unauthorised persons, modified or subject to unauthorised disclosure.

These steps include security access to Aruma IT network, password protection for access to databases and electronic file locations, securing paper-based files containing personal information in locked cabinets and physical access restrictions.

For further information on I.T. security refer to the following Policy & Practice Manuals:

- Access, Security & Controls Policy;
- Network System Data Security Policy; and
- Password Policy.

Personal information contained in physical files will be managed under the guidance of our Archiving & Records Management Policy and Practice Manual, that is:

- files will be stored, retained and disposed of;

- files that are no longer current or requiring access will be archived; and
- files that have expired beyond the required retention period for record keeping will be permanently destroyed.

5.12 APP 12: Access

5.12.1 APP 12 regulates the circumstances in which an individual may obtain access to their personal information.

5.12.2 Individuals will often request access to their information if, for example, they wish:

- *to know what information the entity holds about them; or*
- *to transfer their records or information to a new service provider.*

Aruma's Practice Guidelines:

If a person asks for access to their personal information held by Aruma, we will allow access, unless there is a reason under the Privacy Act or any other law not to give access to the information. Reasons for restrictions to access include:

- A serious threat to the life, health or safety of any individual, or to public health/safety;
- It would impact the privacy of other individuals;
- The request is frivolous or vexatious;
- The information relates to existing or anticipated legal proceedings;
- It would prejudice negotiations with the individual;
- It would be unlawful;
- Denying access is authorised by law;
- Enforcement related activities may be prejudiced; or
- Evaluative information generated within Aruma in connection to a sensitive decision-making process may be revealed.

Employees should direct requests for access to personal information to their line manager. Requests for release of personal information by, or to, a third party should be directed to the Chief Privacy Officer via post to Aruma's PO Box 49, FRENCHS FOREST NSW 2061 or via email: privacy@aruma.com.au.

A response to the request for access will be provided within a reasonable time frame, determined by the extent of information to be accessed, and will give access in a way that

meets both its needs and those of the individual, including the use of a mutually agreed intermediary.

Often requests for access will be received via agents or authorised representatives, such as lawyers and family members.

Documents may be provided to such representatives, provided that the person's authority to act as agent or authorised representative is verified, for example, where the representative is:

- a family member, consent (implied is considered suitable) is provided by the individual for the said family member to act;
- Power of Attorney – the document granting the power is provided/sighted;
- a solicitor – the individual confirms the solicitor has authority to act on their behalf; and
- the representatives' identity is verified.

Prior to providing an individual or their representative with access to their personal information, assessment should be made as to possible breach of privacy for any other individual, or all other names or alternative identifying information should be redacted from the data prior to access, unless explicit consent is obtained from each of the other individuals able to be identified.

Aruma will not charge a fee for access to read personal information but may impose a fee to cover costs of photocopying or file extraction. Such fees, where imposed, will be on a cost basis.

If Aruma is unable to provide access to the information in the way requested by the person, we will take steps to give access in a way that meets both its needs and those of the person.

If Aruma does not agree to the request for access to personal information, we will advise the person in writing of the reason/s why.

Aruma may refuse access if giving access would have an unreasonable impact on the privacy of other individuals, the information to be accessed cannot be reasonably de-identified, providing access would be unlawful, or the information relates to existing or anticipated legal proceedings between Aruma and the individual. Access to information may also be denied if Aruma has reason to suspect unlawful activity, misconduct or the request is deemed frivolous or vexatious.

Further advice or information can be obtained from the Australian Information Commissioner by calling 1300 363 992 or by email: enquiries@oaic.gov.au

5.13 APP 13: Correction of Personal Information

5.13.1 APP 13 states that entities must take reasonable steps to correct personal information that it holds if:

- *it is satisfied that the information is inaccurate, out of date, incomplete, irrelevant or misleading; or*
- *the individual requests the entity to correct the information.*

Aruma's Practice Guidelines:

Aruma will take reasonable steps to correct personal information that it holds if:

- it is satisfied that, considering the purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or
- the person requests that Aruma corrects the information.

If Aruma is asked to correct personal information, it will respond to the request in a reasonable time. Aruma does not impose any fees or charges for correcting personal information.

If Aruma refuses or is unable to comply with a request to correct personal information, they will give written notice to the person advising the reason why they are unable to comply with the request.

6 APP Exemptions

Employee Records

6.1 The Privacy Act does not apply to employee records, provided that they are used purely for employment-related purposes. This includes records of employee engagement, health, training, disciplining, termination, performance, conduct work hours, salary, trade union memberships and leave records.

6.2 Note that information gathered during recruitment processes are not covered by the employee record exemption and should be treated as per the principles of this PPM.

6.3 Regardless of the exemption in the Privacy Act, Aruma treats employee records in the same way as it deals with any other private information as documented above, excluding access to confidential performance related records.

Newsletters

6.4 The Privacy Act contains a 'journalism' exemption for organisations that covers newsletters. Newsletters generally only contain "good news" stories that rarely give rise to privacy issues but are subject to certain requirements being met.

7 Other Privacy Practice Guidelines

Children

7.1 The Privacy Act affords Children the same privacy rights as adults. An assessment should be made of a child's competence to make their own decisions in relation to matters contained within this document. As a general principle, the Privacy Commissioner has stated that an individual between the ages of 15-18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed.

Complaints or Concerns in relation to Privacy

7.2 If you have a complaint in relation to privacy, it should be made in writing, directed to:

Chief Privacy Officer
Aruma
PO Box 93, Frenchs Forest NSW 1640
Or via email: privacy@aruma.com.au

7.3 You should expect an acknowledgement within 7 days of the complaint or concern being received. You will be advised of how your complaint or concern will be dealt with.

7.4 Your complaint or concern will be investigated by the Chief Privacy Officer in consultation with the Chief Executive.

7.5 You will receive written advice of the response to your concern or complaint, or advice of further processes required, within 28 days.

7.6 If the response is not acceptable to you, we may suggest conciliation or arbitration on the matter. You may also make a formal complaint to the Australian Information Commissioner by calling 1300 363 992 or by email: enquiries@oaic.gov.au.

Confidentiality

7.7 Employees, carers, contractors or volunteers who may have access to personal and sensitive information in the course of their duties or dealings with Aruma, are bound by their commitment to confidentiality.

7.8 Breaches of confidentiality will be dealt with in accordance to the conditions of engagement or appointment of those individuals and Aruma's Policy.

Notifiable Data Breaches (NDB) Scheme

7.9 The passage of the *Privacy Amendment (Notifiable Data Breaches) Act 2017* established the Notifiable Data Breaches (NDB) scheme in Australia.

7.10 The NDB scheme obligates Aruma to notify individuals whose personal information is

involved in a data breach that is likely to result in serious harm. This notification must include recommendations about the steps individuals should take in response to the breach. The Australian Information Commissioner (Commissioner) must also be notified of eligible data breaches.

7.11 Guidance on Aruma's obligations under the NDB, can be accessed in the DRAFT Incident Reporting PPM.

Privacy Breaches (VIC)

7.12 In Victoria, Aruma is required to report all customer related privacy incidents to the department within one business day of becoming aware of, or being notified of, a possible privacy incident, or within one business day of an allegation being made of a potential breach.

7.13 A privacy incident may be a breach or possible breach or a 'near miss'.

7.14 Privacy incidents must be reported via the online privacy incident report form, which captures details relating to:

- the privacy incident;
- the customers impacted;
- the immediate risks;
- how the incident is being managed and if a breach has occurred, how it is being contained; and
- information relating to security and breaches.

7.15 Further information and resources regarding how to access and use the privacy incident report form is accessible at: at: https://dhhs.vic.gov.au/publications/privacy-policy and in Section 10 'Instruction: Complete the privacy incident report form' of the Privacy Incident Report Form - User Guide for Funded Agency Staff Members.

7.16 Once the report is submitted, Aruma's Chief Privacy Officer will receive a confirmation email and a reference number.

7.17 The report will be received by the divisional privacy officer and directed to the funded organisation's contract manager within the department (i.e. local engagement officer or program advisor), who will work with Aruma Operational General Manager to manage the incident as required by the Privacy Policy.

7.18 Under the Victorian Client Incident Management System (CIMS), a privacy breach that

impacts a client may need to be reported as a client incident under CIMS as well as through a privacy incident report (Further information may be accessed via the Client Incident Management Guide or Aruma Notifiable Events Policy).

Privacy Impact Assessments

7.19 Aruma encourages the completion of a privacy impact assessment during the early stages of any project that involves the collection, handling, storage or sharing of information. Undertaking a privacy impact assessment is aimed to assist Aruma to:

- describe how personal information flows in a project;
- analyse the possible impacts on individuals' privacy;
- identify and recommend options for avoiding, minimising or mitigating negative privacy impacts;
- build privacy considerations into the design of a project; and
- achieve the project's goals while minimising the negative and enhancing the positive privacy impacts.

7.20 A guide to completing a privacy impact assessment can be found on the OAIC website at: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments

Privacy of Deceased Individuals

7.21 The *Privacy Act* regulates the handling of personal information about individuals. Section 6 of the Act defines an individual as 'a natural person'. The *Privacy Act* does not cover genetic information about deceased persons.

7.22 Although in principle the Privacy Act does not apply to deceased persons, Aruma will take each request for release on its merit and where appropriate only release to, or with authority of, a person listed as the next-of-kin or person responsible.

Resources Relevant to this Policy and Practice Manual

8 QMS policies, procedures and/or forms

Decision Making & Choice PPM

Privacy Dignity and Confidentiality PPM

Code of Conduct

Advocacy, Guardianship & Consent PPM

Consent Form

Management of Records and QMS Documents PPM

(I.T.) Access, Security & Controls Policy

(I.T.) General Network Systems Data Security Policy

(I.T) Password Policy

9 Legislation, external requirements and oversight bodies

Commonwealth:

Privacy Act (Cth) 1988
Australian Privacy Principles (APP) – *replaced National Privacy Principles 12Mar14*

ACT:

Information Privacy Act 2014 (ACT)
Health Records (Privacy & Access) Act 1997 (ACT)
Human Rights Act 2004 (ACT)

NSW:

Privacy & Personal Information Protection Act 1998 (NSW)
Health Records & Information Privacy Act 2002 (NSW)
Workplace Surveillance Act 2005 (NSW)
Surveillance Devices Act 2007 (NSW)

QUEENSLAND:

Information Privacy Act 200 (QLD)
Qld Health, Quality & Complaints Commission Act 1992 (QLD)
Invasion of Privacy Act 1971 (QLD)

VICTORIA:

Information Privacy Act 2000 (VIC)
Health Records Act 2001 (VIC)
Surveillance Devices (Workplace Privacy) Act 2006 (VIC)
Charter of Human Rights and Responsibilities Act 2006 (VIC)

Privacy and Data Protection (PDP) Act 2014 (VIC)

10 External resources

Office of the Australian Information Commissioner – OAIC www.oaic@.gov.au